Gruppo
Banca europea per
gli investimenti

Banca europea per gli investimenti

Procedure d'indagine

PROCEDURE APPLICABILI ALLO SVOLGIMENTO DELLE INDAGINI DELLA DIVISIONE INDAGINI SULLA FRODE ALLA DIREZIONE ISPEZIONE GENERALE DEL GRUPPO BEI («Procedure d'indagine»)

INDICE

A) Introduzione

1. Il presente documento enuncia le procedure applicabili allo svolgimento delle indagini condotte dalla Divisione Indagini sulla frode della Direzione Ispezione generale (IG/IN) del Gruppo Banca europea per gli investimenti (BEI) [1].

2. Le procedure stabilite nel presente documento:
   a. devono leggersi in parallelo alla «Politica di prevenzione e di dissuasione di pratiche vietate nelle attività della Banca europea per gli investimenti» (Politica antifrode);
   b. si applicano a tutte le indagini svolte da IG/IN nella BEI e nel quadro delle sue attività; e
   c. si applicano al FEI, pur con le dovute modifiche, per tenere conto della sua diversa struttura di *governance*.

B) Scopo e natura di un'indagine

3. La Divisione Indagini sulla frode (IG/IN) dell'Ispezione Generale della BEI conduce indagini che hanno lo scopo di esaminare e di verificare la fondatezza delle segnalazioni e delle accuse di casi sospetti di pratica vietata, dannosa per le attività della BEI, oppure di casi sospetti di cattiva condotta (ovvero di comportamento disonesto o illegale, colpa o dolo) che coinvolgono membri degli organi dirigenti o del personale della BEI. La Divisione ha anche il compito di comunicare le conclusioni raggiunte dall'indagine e di formulare le opportune raccomandazioni in merito [2].

4. Tutte le indagini condotte da IG/IN sono di tipo amministrativo.

C) Ricezione e registrazione dei dati riguardanti una segnalazione o un'accusa di caso sospetto di irregolarità

5. La Divisione IG/IN si occupa dell'accettazione delle segnalazioni di casi di sospetta corruzione, frode, collusione, coercizione, ostruzionismo, riciclaggio di denaro e finanziamento del terrorismo (pratiche che nel loro insieme sono definite «pratiche vietate [3]») emananti da qualsiasi fonte all'interno o al di fuori della BEI, e si occupa anche dell'accettazione delle denunce provenienti da fonti anonime o riservate. IG/IN può anche aprire un fascicolo di sua spontanea iniziativa, ad esempio all'occasione di articoli presenti nella stampa che si riferiscono a casi di pratiche vietate. IG/IN risponde a tutti questi tipi di segnalazione secondo le modalità enunciate nei paragrafi seguenti.

6. Se il denunciante è anonimo e insiste ad essere protetto dall'anonimato, IG/IN gli o le richiede di rimettersi in contatto con IG/IN a una data successiva, a un giorno e

[1] La Divisione IG/IN amministra le procedure conformemente, e fatta salva, la decisione del 27 luglio 2004 del Consiglio dei governatori riguardante la cooperazione tra la BEI e l'OLAF.

[2] Il Comitato di deontologia e conformità (*Ethics and Compliance Committee*) è incaricato di valutare i conflitti d'interesse riguardanti un membro del Comitato direttivo o del Consiglio di amministrazione.

[3] La definizione di «pratica vietata» è fornita nella politica antifrode della BEI, disponibile al seguente indirizzo: EIB's Anti-Fraud Policy

un'ora concordati precedentemente per rispondere ad altre domande che potrebbero scaturire da un'analisi preliminare del caso.

7. Il Capo della Divisione IG/IN registra senza indugio i dati e le informazioni raccolte nel sistema di gestione dei casi della Divisione. I dati comprendono, se possibile:
   a. la data di ricevimento delle informazioni;
   b. l'identità dell'autore della segnalazione o dell'accusa, se è stata resa nota;
   c. una sintesi delle informazioni contenute nella segnalazione o nell'accusa, tra cui il tipo di presunto atto illecito o di presunta cattiva condotta (ad esempio, la sostituzione di un prodotto o la manipolazione delle gare di appalto) e le parti che sono sospettate di coinvolgimento;
   d. il nesso eventuale esistente tra tale presunto atto e la BEI o l'attività della BEI, compresa la descrizione e l'ubicazione del progetto o dell'operazione interessata;
   e. qualsiasi altra informazione che viene considerata rilevante per IG/IN;
   f. l'attribuzione del nome e del numero al fascicolo in questione, per facilitarne la tracciabilità; e
   g. la preparazione e l'assegnazione del fascicolo d'indagine a uno o a più funzionari/ investigatori.

8. Se il Capo della Divisione IG/IN decide che i contenuti delle informazioni ricevute non hanno rapporto con la BEI oppure che si tratta di un caso *de minimis,* egli registra prontamente la decisione di archiviazione del caso nel sistema di gestione delle pratiche motivando che, *prima facie*, la segnalazione non costituisce un caso. L'elenco dei casi archiviati senza seguito d'indagine è presente nella relazione annuale sulle indagini elaborata dalla Divisione IG/IN.

9. Il Capo della Divisione IG/IN mette a disposizione, su richiesta, le informazioni riguardanti la segnalazione o l'accusa e la sua valutazione a disposizione delle parti competenti (il Presidente e il Vicepresidente responsabile delle indagini, il Segretario generale, il Comitato di verifica, l'OLAF e i revisori esterni.)

D) Notifica all'OLAF e coinvolgimento dell'Ufficio

10. (i) *Nel caso di indagini esterne:* se il Capo della Divisione IG/IN considera fondato il sospetto che si tratti di un caso di pratica vietata nel contesto di un progetto finanziato dalla BEI o di una sua attività, ne informa prontamente L'Ufficio europeo per la lotta antifrode (OLAF) e gli trasmette le necessarie informazioni [4]. IG/IN prosegue l'indagine amministrativa in attesa della decisione dell'OLAF di aprire un fascicolo d'indagine. Se l'OLAF decide di avviare un'inchiesta, IG/IN si terrà in stretta cooperazione con i funzionari investigatori dell'OLAF incaricati del caso. Se invece l'OLAF, per una qualsivoglia ragione, decide di non avviare un'inchiesta, il Capo di IG/IN può comunque decidere di portare avanti la sua indagine.

    (ii) *Nel caso di indagini interne:* se il Capo della Divisione IG/IN ritiene fondato il sospetto che si tratti di un caso di cattiva condotta o di illecito da parte di un membro degli organi dirigenti o del personale della BEI/FEI, egli ne informa senza indugio l'OLAF e gli trasmette le informazioni necessarie. Se l'OLAF decide di avviare un'indagine interna, la Divisione IG/IN offre agli inquirenti dell'OLAF tutta l'assistenza necessaria. Il sostegno si può concretizzare con il

[4] V. Regolamenti 1074/1999 (Euratom) e 1073/1999 (CE): http://eur-lex.europa.eu/LexUriServ/site/en/oj/1999/l_136/l_13619990531en00010007.pdf

dare accesso ai dati personali e ai dati elettronici disponibili nei sistemi della Banca, preparare e partecipare a colloqui ecc. Se l'OLAF decide, per un qualsivoglia motivo, di non avviare un'indagine, il Capo della Divisione IG/IN può tuttavia decidere di portare avanti l'indagine.

E) Svolgimento dell'indagine

(i) In via generale

11. Per quanto fattibile, IG/IN deve mettersi in contatto con il denunciante per avvisarlo della ricezione della denuncia e per ottenere informazioni più circostanziate sulla segnalazione o accusa, come ad esempio:
    a. una descrizione completa del presunto illecito o trasgressione (ovvero comportamento scorretto, colpa o dolo);
    b. il legame presunto con i finanziamenti della BEI oppure con sue altre attività e una stima dell'entità dei fondi a rischio;
    c. i nomi, le ubicazioni ovvero gli estremi delle persone o delle entità coinvolte o che potrebbero avere altre informazioni in merito all'accusa;
    d. le date in cui si situano i fatti;
    e. l'ubicazione e la descrizione di eventuali documenti, dati o registri in archivio pertinenti al caso;
    f. gli elementi che hanno portato il denunciante ad essere a conoscenza dei fatti e il suo scopo/movente;
    g. eventuali preoccupazioni riguardo alla possibilità di ritorsioni o aspetti collegati alla sicurezza personale; e/o
    h. qualsiasi altra informazione pertinente.

12. Appena possibile, dopo aver inserito i dati pertinenti nel sistema di gestione dei casi, IG/IN deve cercare conferma del fatto che il caso presunto di violazione, colpa o illecito o di cattiva condotta effettivamente coinvolge un'operazione della BEI (compresi i progetti finanziati dalla BEI nell'UE o nei Paesi terzi dell'UE), oppure un membro degli organi dirigenti o del personale.

13. Nell'ambito di un primo esame dei documenti del caso, IG/IN cerca di determinare se:
    a. la presunta trasgressione (violazione, illecito, colpa o dolo) oppure cattiva condotta rappresenta un rischio sufficientemente rilevante [5] per la BEI da giustificare l'apertura di un'indagine; e
    b. se un indagine è effettivamente realizzabile, tenuto conto dell'aspetto temporale dei fatti in questione, della specificità delle informazioni ricevute, della disponibilità della documentazione o di testimoni necessari e di altre informazioni pertinenti.

14. IG/IN cerca peraltro di valutare obiettivamente l'attendibilità della segnalazione o dell'accusa. A tale proposito, tra i vari passi da compiere, può essere utile fare riferimento a:
    a. un progetto, un finanziamento o ad altri documenti, fascicoli o dati della BEI;
    b. eventuali segnalazioni o accuse antecedenti, che interessano le parti sospettate e che sono state ricevute dalla BEI o dall'OLAF;
    c. verifiche contestuali nelle banche dati sulle imprese e nelle mediateche; e
    d. altre fonti d'informazione pertinenti.

[5] Tra i fattori da valutare vi è il rischio operativo, finanziario e di reputazione per la BEI e per le sue attività.

(ii) Fonti d'informazione

15. In sede d'indagine, IG/IN può:
    a. esaminare, secondo i casi, la documentazione conservata presso le parti coinvolte quali i prenditori, promotori, contraenti, subappaltatori, consulenti, fornitori e terzi, nel rispetto delle disposizioni del contratto di prestito della BEI in questione e della Guida all'aggiudicazione degli appalti della BEI;
    b. svolgere controlli e verifiche sul posto di qualsiasi opera, struttura, locale o altri beni d'interesse ai fini di un'indagine, e registrare i risultati raccolti con materiale fotografico o altro;
    c. interrogare testimoni e/o le persone interessate; e/o
    d. consultare altre parti, tra cui quelle che conducono *audit* o indagini pertinenti.

16. Più precisamente, le fonti d'informazioni utili a un'indagine comprendono (senza peraltro limitarsi a):
    a. documenti di qualsiasi tipo;
    b. dati elettronici;
    c. dati in supporto video, audio o fotografico;
    d. i risultati d'ispezioni e di controlli;
    e. le osservazioni dell'inquirente; e
    f. prove testimoniali (scritte e orali), comprese quelle della persona oggetto dell'indagine.

17. IG/IN non ricompensa con denaro un testimone per le informazioni date. Può peraltro rimborsare un testimone per le spese ragionevoli incorse in seguito alla sua cooperazione con IG/IN.

18. IG/IN può ricorrere alla consulenza o all'assistenza di altri dipartimenti della BEI, e/oppure di consulenti e di periti esterni per ottenere assistenza nel quadro di un'indagine.

(iii) Documenti

19. Per quanto riguarda i documenti che possono essere richiesti come elementi di prova ammissibili nei procedimenti amministrativi o di altro tipo, IG/IN deve:
    a. tentare d'identificare e utilizzare il documento originale oppure, se risulta difficoltoso procurarselo a condizioni ragionevoli, copie affidabili;
    b. conservare, in modo ragionevolmente pratico, tutti i documenti nello stato in cui sono stati ricevuti; e
    c. essere in grado d'identificare la data e il luogo in cui il documento è stato ottenuto e il latore stesso.

(iv) Dati elettronici e personali

20. Per quanto concerne i dati elettronici, IG/IN deve:
    a. ottenerli
        i. dalla fonte più affidabile a disposizione, a condizioni ragionevoli, ovvero dal luogo o dal sito che conserva i dati più completi, precisi e aggiornati;
        ii. nel modo in cui, per quanto sia ragionevolmente fattibile, sia protetta l'integrità, si garantisca che i dati non siano ritoccati, manipolati o corrotti in qualsiasi modo; e

b. essere in grado d'identificare la data e il luogo in cui il documento è stato ottenuto e il latore stesso.

21. La Divisione IG/IN ha facoltà di consultare e di copiare dati elettronici (tra cui email/dati creati, copiati o ricevuti da un membro degli organi decisionali o del personale della BEI, utilizzando un qualsiasi componente dei sistemi informatici della BEI) e dati personali potenzialmente pertinenti, munita del nulla osta scritto da parte del Direttore del Personale del Responsabile della protezione dei dati della BEI. Ciò inoltre deve avvenire nel rispetto della normativa applicabile, delle regole, dei regolamenti, delle politiche e procedure in vigore, nonché del Protocollo applicabile alle procedure di informatica forense (V. Allegato 1). Intervenendo in tal modo, IG/IN informa il Direttore del Personale e il Responsabile della protezione dei dati della BEI dei motivi che giustificano questo accesso ai dati ai fini delle indagini, sempre nella tutela dell'identità delle fonti e delle persone coinvolte.

(v) Informazioni raccolte durante i colloqui

22. Le procedure seguenti si applicano a tutti i colloqui svolti da IG/IN all'interno o al di fuori della BEI, e in particolare al colloquio/prova testimoniale di una persona coinvolta in un'indagine:
    a. I colloqui si svolgono
        i. nella lingua con la quale il testimone e il funzionario inquirente hanno più dimestichezza, oppure con l'aiuto di un interprete; e
        ii. in presenza di due funzionari inquirenti, se IG/IN lo considera opportuno.
    b. Prima dell'inizio del colloquio, la persona interrogata è informata del suo diritto di farsi assistere da una persona di sua scelta e che il verbale del colloquio può essere un elemento di prova ammissibile nei procedimenti amministrativi, disciplinari o di altro simile tipo;
    c. IG/IN redige senza indugio il verbale del colloquio;
    d. IG/IN può, a sua discrezione, fornire al testimone del colloquio una copia del verbale per controllo e firma, soprattutto nei casi in cui la sua testimonianza potrebbe essere fondamentale su certi punti essenziali;
    e. una copia del verbale del colloquio dev'essere sempre inviata ai membri degli organi dirigenti o del personale sospettati di cattiva condotta o di illecito, per controllo e firma; e
    f. i colloqui possono essere registrati per via elettronica, sempreché il testimone ne sia informato e abbia dato l'accordo.

F) Ostruzione di un'indagine

23. *Nelle indagini interne*: se le conclusioni dell'indagine indicano che un membro degli organi dirigenti o del personale:
    a. ha deliberatamente dichiarato il falso a IG/IN in una segnalazione, accusa o durante un'indagine;
    b. è venuto meno all'obbligo di cooperare a un'indagine, come richiedono il codice di condotta applicabile e la politica antifrode in vigore alla BEI; oppure
    c. ha tentato in un qualsiasi modo di perturbare, impedire o ostacolare l'indagine;

IG/IN ne deve informare il Presidente e il Direttore del Personale che valuteranno misure disciplinari appropriate e proporzionate.

24. *Per le indagini esterne*: Le pratiche di ostruzionismo, come vengono definite nelle procedure di esclusione della BEI, consistono in un'azione che comporta (a) distruggere, falsificare, alterare o nascondere deliberatamente materiale utile alle indagini; e/o minacciare, molestare o intimidire qualsiasi parte al fine d'impedirle di riferire circa elementi di sua conoscenza utili alle indagini o di condurre le stesse, ovvero (b) atti volti ad impedire materialmente l'esercizio dei diritti contrattuali di verifica da parte della BEI o di accedere alle informazioni o ai diritti che ogni autorità bancaria, regolamentare o esaminatrice o altro organo equivalente dell'Unione europea o dei suoi Stati membri abbia in forza di legge, regolamento o trattato o in ragione di qualsiasi accordo siglato dalla BEI al fine di implementare tale legge, regolamento o trattato.

    Qualsiasi persona fisica, organizzazione, società o entità che è coinvolta in una pratica vietata (tra cui quella di ostruzionismo) può essere soggetta ad esclusione, in forza delle procedure di esclusione della BEI.

G) Chiusura di un'indagine e conclusioni

25. L'onere della prova applicabile a IG/IN, per giungere alla conclusione che una segnalazione o accusa di caso presunto di trasgressione o d'illecito sia motivata, corrisponde a quando tutti i dati informativi, nel loro insieme, dimostrano che le conclusioni dell'indagine sono più probabili che improbabili.

26. Le conclusioni di un'inchiesta devono basarsi sui seguenti elementi:
    a. informazioni concrete, più affidabili possibile, nonché deduzioni e conclusioni che emergono da fatti accertati; per quanto fattibile, documenti, dati elettronici, tests e risultati di verifiche autentificati dagli autori, destinatari o depositari, o da altre persone che direttamente posso testimoniare sulla loro autenticità;
    b. per quanto fattibile, dichiarazioni di testimoni che hanno conoscenza diretta dei fatti e delle circostanze in questione;
    c. informazioni che sono state corroborate, il più quanto possibile, da altre fonti d'informazione affidabili, tra cui da altri testimoni, da documenti o dati;
    d. informazioni ragionevoli credibili sia a carico che a discarico.

27. Le conclusioni delle indagini possono includere certi elementi complementari forniti da IG/IN, quali:
    a. osservazioni su come è percepita la credibilità e il comportamento di un testimone, e della persona oggetto d'indagine;
    b. raccomandazioni sul corso più opportuno da prendere per trattare i temi oggetto d'indagine, oppure le questioni più ampie di natura politica che sono state identificate nel corso dell'indagine. I servizi della BEI informano IG/IN delle misure prese per attuare tali raccomandazioni nei tempi previsti.

28. Laddove il Capo della Divisione IG/IN reputi che la segnalazione o accusa di caso presunto di violazione o d'illecito sia motivata e che occorre un intervento successivo, registra o documenta opportunamente tale conclusione e ne riferisce alle autorità competenti all'interno della BEI stessa o al suo esterno, affinché siano prese ulteriori misure necessarie.

29. Qualora il Capo della Divisione IG/IN reputi, a seguito di un'indagine ragionevole, che la segnalazione o accusa di caso presunto di violazione o

d'illecito non sia motivata, registra e documenta questa conclusione nel sistema di gestione dei casi e il caso è chiuso. Se durante l'esame o l'inchiesta nel merito della segnalazione o accusa di caso presunto di violazione o d'illecito giungono all'attenzione di IG/IN informazioni che possono essere pertinenti ad altri organi all'interno o all'esterno della BEI, il Capo di IG/IN le può inviare, sempreché siano pienamente rispettate le regole in vigore di tutela dei dati.

30. Il Capo della Divisione IG/IN ha la facoltà di riaprire un caso già chiuso se riceve nuove informazioni credibili, oppure se ciò è giustificato da altre circostanze che emergono.

H) Protezione dei dati – Diritti individuali e doveri d'informazione

(i) Principi generali

31. Come precisa la politica antifrode, il trattamento dei dati personali - nell'ambito delle presenti procedure - deve conformarsi ai principi e alle regole di cui dispongono i regolamenti che sui applicano alla Banca [6] e ai pareri pertinenti emessi dal Garante europeo della protezione dei dati. Tutte le persone coinvolte hanno il diritto di accedere, rettificare e (in taluni casi) bloccare dati che le riguardano consultando il responsabile del trattamento dei dati [7]. Esse possono allo stesso modo e in qualsiasi momento consultare il Garante europeo della protezione dei dati [8].

(ii) Rispetto dei diritti delle persone interessate

32. Qualsiasi persona coinvolta in un'indagine (sia come sospettata, testimone o altro), dev'essere informata del trattamento dei dati personali che avviene nel corso di una procedura d'indagine condotta dalla Divisione IG/IN, in forza degli articoli 11 e 12 del Regolamento (CE) n. 45/2001 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali, a meno che non si applichino le limitazioni enunciate all'articolo 20 del suddetto regolamento, nel cui caso IG/IN dovrà regolarmente riesaminare se tali limitazioni sono sempre applicabili, oppure se il soggetto a cui i dati si riferiscono deve ricevere una notifica d'indagine in corso.

(iii) Principio della qualità dei dati personali

33. La Divisione IG/IN garantisce il rispetto del principio di qualità dei dati, come dispone l'articolo 4 del Regolamento (CE) n. 45/2001, secondo cui i dati personali devono essere esatti e, se necessario, aggiornati, ma anche adeguati, pertinenti e non eccedenti rispetto alle finalità dell'indagine per le quali vengono raccolti o successivamente trattati. Inoltre, i dati devono essere trattati in modo corretto e lecito e solo per finalità determinate, esplicite e legittime.

---

[6] In particolare, devono conformarsi al Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (Gazzetta Ufficiale L8/1 del 12 gennaio 2001).

[7] Il responsabile del trattamento dei dati è consultabile al seguente indirizzo: investigations@eib.org

[8] Il garante europeo della protezione dei dati è consultabile al seguente indirizzo: www.edps.europa.eu

34. La valutazione delle informazioni da parte della Divisione IG/IN deve basarsi sull'informazione concreta più affidabile che sia a disposizione, nonché su fatti accertati.

(iv) Trasferimento dei dati personali al di fuori della BEI

35. La Divisione IG/IN ha la possibilità di trasferire dati personali ai suoi partner operativi, siano essi istituzioni, organi o organismi dell'UE, come ad esempio l'OLAF, le autorità degli Stati membri, le autorità dei Paesi terzi, oppure le organizzazioni internazionali, durante lo svolgimento delle sua attività operative. Ciò può avvenire per iscritto, per posta elettronica, oralmente (con telefonate, colloqui/contatti personali), oppure con qualsiasi altro mezzo. Questi tipi di trasferimenti devono essere proporzionati, tenendo conto della natura dei dati raccolti e successivamente trattati; il trasferimento dei dati è consentito unicamente se i dati sono necessari per il legittimo esercizio delle funzioni che rientrano nelle competenze del destinatario. Nell'esecuzione di un trasferimento di dati personali nell'ambito di un caso, la Divisione IG/IN provvede a che siano assicurate disposizioni standard e adeguate di protezione dei dati.

I) Altri aspetti

(i) Relazione sullo stato delle attività

36. La Divisione IG/IN provvede a inviare, trimestralmente e per conoscenza, una Relazione sullo stato delle attività al Comitato direttivo, al Comitato di verifica e all'OLAF.

(ii) Politica di conservazione dei dati

37. Tutti i documenti e informazioni riguardanti i casi trattati sono conservati in modo sicuro e riservato dalla Divisione IG/IN per una durata di almeno cinque anni e fino a un massimo di dieci anni a decorrere dalla data di chiusura del caso.

38. Per quanto concerne le segnalazioni o accuse di casi presunti di violazione o d'illecito che sono archiviate, ovvero, a cui la Divisione IG/IN non ha dato seguito con l'apertura di un'indagine (segnalazioni che, *prima facie*, non costituiscono un caso), oppure per quanto riguarda i casi chiusi a seguito di segnalazioni o accuse considerate immotivate (i casi privi di fondamento), la documentazione e le informazioni pertinenti sono conservate fino a un massimo di cinque anni a decorrere dalla decisione di non procedere con l'apertura di un'indagine oppure di chiusura del caso.

(iii) Segnalazione o accusa di caso presunto di cattiva condotta a carico di un membro di IG/IN

39. Qualora necessario, l'Ispettore generale prenderà disposizioni specifiche caso per caso, per indagare in merito a una segnalazione o accusa di caso presunto di cattiva condotta, trasgressione o illecito a carico di un membro della Divisione IG/IN.

(iv) Aggiornamento delle procedure d'indagine

40. Come avviene nel caso della politica antifrode, le presenti procedure sono modificate e aggiornate, qualora necessario e opportuno, a seguito di:
    a. modifiche al testo intitolato «Politica di prevenzione e di dissuasione di pratiche vietate nelle attività della BEI»;
    b. esperienza maturata nell'applicazione delle procedure;
    c. evoluzione delle migliori pratiche nella materia;
    d. qualsiasi altro cambiamento che la BEI giudica necessario e appropriato.

Allegato 1: Protocollo della BEI riguardante le procedure d'informatica forense

1. Definizione dell'attività di analisi d'informatica forense

L'analisi d'informatica forense consiste in una perizia tecnologica sistematica delle attrezzature elettroniche e dei loro contenuti, onde raccogliere informazioni che possono essere utili ai fini di un'indagine in corso e che possono eventualmente far parte di un fascicolo di prove forensi in un eventuale successivo procedimento giudiziario.

2. Principi nell'attività d'informatica forense

2.1 Non sono state ad oggi pubblicate procedure formali d'informatica forense che siano state concordate a livello intergovernativo, internazionale o europeo.

2.2 Nei casi in cui le indagini competono all'OLAF, la BEI normalmente si affida alle competenze, ai periti e alle attrezzature dell'Ufficio stesso. Rispetterà rigorosamente le procedure concordate con l'OLAF. Nel caso eccezionale in cui non compete all'OLAF condurre un'indagine, oppure se l'Ufficio decidesse di non indagare, la BEI può ricorrere all'assistenza di società private di comprovata esperienza. La BEI aderisce in questi casi ai quattro grandi principi che l'Associazione britannica dei capi della polizia segue (*Association of Chief Police Officers – ACPO*) nel campo dell'informatica forense:

Principio n. 1: I dati conservati su computer o supporti di memoria, che potrebbero rilevare ai fini di un eventuale procedimento giudiziario, non possono essere modificati da azioni degli organismi preposti al controllo o dei loro agenti.
Principio n. 2: in circostanze eccezionali, una persona che ritiene necessario accedere ai dati originali conservati su computer o supporti di memoria, deve essere competente ad accedervi, e deve fornire prove che dimostrino la pertinenza e le conseguenze dell'azione. (Inoltre, la persona che accede ai dati originali conservati su computer o supporti di memoria deve giustificare la necessità dell'accesso e ottenere l'approvazione del responsabile della protezione dei dati della BEI prima di effettuare tale azione).
Principio n. 3: è necessario elaborare e conservare una pista di controllo o altre registrazioni di tutti i processi svolti sugli elementi di prova elettronici su supporto informatico. Un terzo indipendente deve poter esaminare tali processi e ripeterli ottenendo gli stessi risultati.
Principio n. 4: la persona incaricata dell'indagine (il funzionario competente) ha la responsabilità generale di assicurare il rispetto della legge e l'applicazione di questi principi.

2.3 Inoltre, la BEI seguirà una metodologia ispirata alle migliori pratiche:

- Qualsiasi attività relativa al sequestro, all'accesso, all'archiviazione o al trasferimento di dati digitali dev'essere pienamente documentata, conservata e disponibile per un riesame.
- L'elemento di prova originale dev'essere acquisito in modo tale da proteggere e preservare l'integrità della prova.

3. Procedure d'informatica forense nei casi in cui l'OLAF non interviene

3.1. *Stabilire obiettivi raggiungibili:* svolgere operazioni e perizie d'informatica forense è anche un compito che richiede un elevatissimo apporto di manodopera, e quindi di risorse. In virtú della complessità delle attività e della scarsità di risorse dedite all'informatica forense, per ottenere la massima efficienza ed efficacia operativa, le operazioni presuppongono la seguente pianificazione:

1. Determinare la specificità del valore aggiunto che si otterrebbe con l'operazione forense. In quali luoghi, secondo quali modalità e tempi i periti forensi possono assistere all'indagine? È un'attività necessaria?
2. Determinare ex ante gli obiettivi raggiungibili. Già in fase d'istruttoria preliminare gli investigatori devono definire con precisione l'ambito dell'operazione prevista. Si può verificare la necessità, in corso d'opera, di dover ottenere altri dati selettivi. L'esame diretto dei dati, laddove possibile, può contribuire a ben definire il perimetro operativo.
3. Realizzare gli obiettivi prefissati, ovvero l'operazione, dev'essere fattibile con le risorse disponibili.
4. Realizzare gli obiettivi prefissati nei tempi previsti. Assicurare che le scadenze siano rispettate, per evitare di compromettere l'intera operazione, ovvero la scadenza del termine legale.
5. Misurare gli esiti dell'acquisizione o del sequestro dei dati, ovvero che siano state accertate le prove a carico o a discarico della persona interessata e riferirne nella relazione conclusiva sul caso.

3.2. *Protezione dei dati*: la persona interessata dev'essere informata per iscritto che la BEI aderisce al disposto del Regolamento (CE) 45/2001 e che, com'è enunciato nella sua politica antifrode e nelle procedure applicabili allo svolgimento delle indagini, garantisce scrupolosamente il rispetto di tutti gli obblighi pertinenti alla protezione dei dati nel corso delle perizie d'informatica forense.

Gruppo
Banca europea per
gli investimenti

Contatti

Per informazioni di carattere generale:

Ufficio Informazioni
+352 4379-22000
+352 4379-62000
info@eib.org

Banca europea per gli investimenti
98-100, boulevard Konrad Adenauer
L-2950 Luxembourg
+352 4379-1
+352 437704
www.eib.org